FACTA UNIVERSITATIS (NIŠ)
Ser. Math. Inform. Vol. 39, No 1 (2024), 177–181
https://doi.org/10.22190/FUMI230812012K
Original Scientific Paper

GENERATORS FOR THE ELLIPTIC CURVE $E_{(p,q)} : y^2 = x^3 - p^2x + q^2$

Mehrdad Khazali[1], Hassan Daghigh[2] and Amir Alidadi[1]

[1] **Department of Mathematics, Higher Educational Complex of Bam, Iran**
[2] **Faculty of Mathematical Sciences, University of Kashan, Iran**

ORCID IDs: Mehrdad Khazali https://orcid.org/0000-0002-7460-6983
Hassan Daghigh https://orcid.org/0000-0002-4242-769X
Amir Alidadi https://orcid.org/0000-0001-9608-0663

Abstract. Let $\{E_{(p,q)}\}$ denote a family of elliptic curves over $\mathbb{Q}$ as defined by the Weierstrass equation $E_{(p,q)} : y^2 = x^3 - p^2x + q^2$ where p and q are both prime numbers greater than 5. As evidence that this has two independent points, we already showed that at least the rank of $\{E_{(p,q)}\}$ is two. In this study, we show that the two independent points are part of a $\mathbb{Z}$-basis for the quotient of $E_{(p,q)}(\mathbb{Q})$ by its torsion subgroup.
Keywords: Independent points, Rank of an elliptic curve, Canonical Height.

1. Introduction

Let $\{E_{(1,m)}\}$ be a family of elliptic curves over $\mathbb{Q}$ as determined by the Weierstrass equation $E_{(1,m)} : y^2 = x^3 - x + m^2$ where m is an integer number greater than 1. Brown and Myers in [2] discovered that this family included two independent points. Fujita and Nara in [3] proved that the two independent points could be extended to form the basis for this family.

Let $\{E_{(n,1)}\}$ be a family of elliptic curves over $\mathbb{Q}$ as defined by the Weierstrass equation $E_{(n,1)} : y^2 = x^3 - n^2x + 1$ where n is an integer number greater than 1. In [1], Antoniewicz provided evidence that this family contained two independent points. Fujita and Nara in [3] showed that the two independent points could be extended to form the basis for this family.

The family of elliptic curves over $\mathbb{Q}$, as described by the Weierstrass equation $E_{(p,q)} : y^2 = x^3 - p^2x + q^2$, where p and q are both prime numbers greater than 5,

Received August 12, 2023, revised: October 25, 2023, accepted: October 25, 2023
Communicated by Mojtaba Bahramian Mail, Amirhossein Nokhodkar Mail and Predrag Stanimirović
Corresponding Author: Mehrdad Khazali. E-mail addresses: mehrdad@bam.ac.ir (M. Khazali), hassan@kashanu.ac.ir (H. Daghigh), alidadi@bam.ac.ir (A. Alidadi)
2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 14G05

is represented by the $\{E_{(p,q)}\}$. We recently proved that the points $P_1 = (0, q)$ and $P_2 = (-p, q)$ are independent points. In this essay, we describe how the two points P_1 and P_2 might be extended and expanded to serve as the basis for this family under particular circumstances. Theorem 1.1 demonstrates the most potent single assertion.

Theorem 1.1. *[Main Theorem]. Let $\{E_{(p,q)}\}$ denote a family of elliptic curves over $\mathbb{Q}$ as defined by the Weierstrass equation $E_{(p,q)} : y^2 = x^3 - p^2x + q^2$ where p and q are both prime numbers greater than 5. If $p > 2\sqrt[4]{2}q$, then $P_1 = (0, q)$ and $P_2 = (-p, q)$ are part of a $\mathbb{Z}$-basis for the quotient of $E_{(p,q)}(\mathbb{Q})$ by its torsion subgroup.*

2. Upper and Lower bound

We continue exploring the idea of canonical height in this section because it is crucial for elliptic curve arithmetic. Point P's canonical height, expressed as

$$\begin{aligned} \hat{h} : E(\mathbb{Q}) &\longrightarrow [0, \infty) \\ P &\longmapsto \begin{cases} \lim\limits_{n\to\infty} \dfrac{h(2^nP)}{4^n} & P \neq \mathcal{O} \\ 0 & P = \mathcal{O} \end{cases} \end{aligned}$$

dose is not suitable for computation. The alternative definition of canonical height offered here with [6] is Tate's height. Therefore, we have

$$\hat{h}(P) = \hat{\lambda}_\infty(P) + \sum_{r|\Delta} \hat{\lambda}_r(P).$$

In fact, the canonical height is the sum of the archimedean local height and the local height, assuming that r is a prime number such that $r \mid \Delta$. We also note that the discriminant of $E_{(p,q)}$ is $\Delta = 16(4p^6 - 27q^4) = 16\Delta'$. We have previously shown that 3 and $5 \nmid \Delta'$. In this article, Δ' is assumed to be square-free. At the moment, we claim that the equation $y^2 = x^3 - p^2x + q^2$ is the global minimum.

Proposition 2.1. *The Weierstrass equation $y^2 = x^3 - p^2x + q^2$ is the global minimum.*

Proof. In view of Lemma 3.1 of [3]. □

Now, we compute $c_4 = 48p^2$, $c_6 = -864q^2$, $b_2 = 0$, $b_4 = -2p^2$, $b_6 = 4q^2$ and $b_8 = -p^4$. The upper and lower bounds of the canonical heights for P_1 and P_2 are established by the following theorems:

Theorem 2.1. *Let $\{E_{(p,q)}\}$ represent a family of elliptic curves over $\mathbb{Q}$ as defined by the Weierstrass equation $E_{(p,q)} : y^2 = x^3 - p^2x + q^2$, where p and q are both prime* *numbers greater than 5. we consider* $P_1 = (0, q) \in E_{(p,q)}(\mathbb{Q})$ *and* $P_2 = (-p, q) \in E_{(p,q)}(\mathbb{Q})$. *If* $p > 2\sqrt[4]{2}q$, *then*

$$\hat{h}(P_1) \leqslant \frac{1}{2}log(p) + \frac{1}{24}log(2^{11}p^4), \quad \hat{h}(P_2) \leqslant \frac{1}{2}log(p) + \frac{1}{6}log(2^{11}p^4).$$

Proof. According to (4.1) of [6], we have

$$H = Max\{4, 2p^2, 8q^2, p^4\}.$$

The theorem's assumption leads to the conclusion that $H = p^4$. To compute the upper bound for canonical height for point P_1 based on Theorem (2.2) of [6], we must apply Equation 2.1.

$$\hat{\lambda}_\infty(P) = \frac{1}{8}\log(|(x^2+p^2)^2 - 8q^2x|) + \frac{1}{8}\sum_{n=1}^{\infty} 4^{-n}\log(|z(2^nP)|). \tag{2.1}$$

Hence, we have

$$\hat{\lambda}_\infty(P_1) \leqslant \frac{1}{2}log(p) + \frac{1}{24}log(2^{11}p^4) = UB1,$$

and so for point P_2. According to Theorem (2.2) of [6], we must apply Equation 2.2.

$$\hat{\lambda}_\infty(P) = \frac{1}{2}\log(|x|) + \frac{1}{8}\sum_{n=0}^{\infty} 4^{-n}\log(|z(2^nP)|). \tag{2.2}$$

Hence, we have

$$\hat{\lambda}_\infty(P_2) \leqslant \frac{1}{2}log(p) + \frac{1}{6}log(2^{11}p^4) = UB2.$$

□

Theorem 2.2. *Let* $\{E_{(p,q)}\}$ *represent a family of elliptic curves over* $\mathbb{Q}$ *as defined by the Weierstrass equation* $E_{(p,q)} : y^2 = x^3 - p^2x + q^2$ *where* p *and* q *are both prime numbers greater than 5. Let* $P \in E_{(p,q)}(\mathbb{Q})$ *be a rational point on* $E_{(p,q)}$. *If* $p > 2\sqrt[4]{2}q$, *then*

$$\hat{h}(P) > \frac{1}{8}log(\frac{p^4}{2}) - \frac{1}{3}log(2) = LB.$$

Proof. We have two scenarios for computing the local height based on Proposition 2.1 and Theorem [6]. The condition $\lambda_2(P) = 0$ occurs if P reduces to a nonsingular point in module 2. Otherwise, P becomes a singular point modulo 2. According to (c) of Theorem (5.2) of [6], we have $\lambda_2(P) = -\frac{1}{3}log(2)$. Next, we show that

$$\hat{\lambda}_\infty(P) \geqslant \frac{1}{8}\log(|(x^2+p^2)^2 - 8q^2x|) \geqslant \frac{1}{8}\log(|p^4 - 16q^4|) > \frac{1}{8}log(\frac{p^4}{2}),$$

therefore

$$\hat{h}(P) > \frac{1}{8}log(\frac{p^4}{2}) - \frac{1}{3}log(2).$$

□

3. Proof of Theorem 1.1

An important theorem applied to prove Theorem 3.1 is Theorem (3.1) of [5].

Theorem 3.1. *Let E be an elliptic curve with a rank of $r \geqslant 2$ over $\mathbb{Q}$. Let P_1' and P_2' be independent points in the $E(\mathbb{Q})$ modulo $E(\mathbb{Q})_{tors}$. Choose a basis $\{Q_1, Q_2, \dots, Q_r\}$ for $E(\mathbb{Q})$ modulo $E(\mathbb{Q})_{tors}$ according to the condition $P_1', P_2' \in \langle Q_1\rangle + \langle Q_2\rangle$. Assume that $E(\mathbb{Q})$ contains no infinite-order point Q with $\hat{h}(Q) \leqslant \lambda$ where λ is a positive real number. Then, index v of the span of P_1' and P_2' in $\langle Q_1\rangle + \langle Q_2\rangle$ satisfies*

$$v \leqslant \frac{2}{\sqrt{3}} \frac{\sqrt{R(P_1', P_2')}}{\lambda}$$

where

$$R(P_1', P_2') = \hat{h}(P_1')\hat{h}(P_2') - \frac{1}{4}(\hat{h}(P_1' + P_2') - \hat{h}(P_1') - \hat{h}(P_2'))^2 < \hat{h}(P_1')\hat{h}(P_2'),$$

thus

$$v \leqslant \frac{2}{\sqrt{3}} \frac{\sqrt{\hat{h}(P_1')\hat{h}(P_2')}}{\lambda}.$$

This has enabled us to demonstrate Theorem 1.1.

Proof. In addition to the fact that $2 \nmid v$ holds true, we support our claim with three theorems: 2.1, 2.2 and 3.1.

The right-hand side of the equation is now established as follows:

$$v \leqslant \frac{2}{\sqrt{3}}.\frac{\sqrt{UB1.UB2}}{LB}.$$

The calculation yields the value $v < 3$ for all prime numbers $p \geqslant 41$. The evidence is therefore persuasive. $\square$

Acknowledgment

We would like to thank the referees for their careful reading and valuable comments.

REFERENCES

1. A. Antoniewicz: *On a family of elliptic curves*, Univ. Iagel. Acta Math. **43** (2005), 21–32.
2. E. Brown and T.M. Bruce: *Elliptic curves from Mordell to Diophantus and back*, The American mathematical monthly **109(7)** (2002), 639-649.
3. Y. Fujita and N. Tadahisa: *The Mordell-Weil bases for the elliptic curve of the form $y^2 = x^3 - m^2x + n^2$*, Publ. Math. Debrecen **92/1-2** (2018), 79-99.

4. M. KHAZALI and D. HASSAN: *Family Of Elliptic Curves* $E(p,q) : y^2 = x^3 - p^2x + q^2$, Facta Universitatis, Series: Mathematics and Informatics **34(4)** (2019), 805-813.
5. S. SIKSEK: *Infinite descent on elliptic curves*, Rocky Mountain J. Math. **25(4)** (1995), 1501–1538. MR1371352.
6. J.H. SILVERMAN: *Computing heights on elliptic curves*, Math. Comp. **51(183)** (1988), 339-358.